UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,567	03/28/2001	Soichi Furuya	520.39632VX1	4795

24956 7590 06/02/2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/818,567	FURUYA ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-12,21-24 and 33-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-12,21-24 and 33-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9 March 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 9 March 2005 with an original application filed 16 February 2001, with acknowledgement of foreign application date of 09 March 2000.

2. Amendments to the claims and abstract are accepted. Claims 9-12, 21-24, and 33-36 are currently pending in this application. Claims 9, 21, and 33 are independent claims.

3. The arguments presented in the amendment are moot due to new grounds of rejection.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 9-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, a computer program. To overcome this 101 rejection applicant needs to amend the independent claim 9 so that a computer is performing the symmetric-key encryption method.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 9-12, 21-24, and 33-36 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. The steps that include: 'a counter and the two pseudo-random number sequences, as well as concatenates the series of ciphertext blocks one after

another sequentially' critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). The subject matter is essential for an understanding of the claimed invention because the claims as written do not provide one an understanding how to use the invention, for example the operation(s), are not defined, in addition it is not clear how many operations are performed, and there is no clear understanding of the order that the operation(s) and encryption are performed.

In the step "outputting a feedback value obtained as a result of operation on said one of said plurality of plaintext blocks and said random number block" the "operation" is not described in the claims or understandable in light of the specification.

Furthermore, in the step "said feedback value being fed back for use in the operation on another one of said plurality of plaintext blocks" because the operation is not described, in addition there is no clear understanding which plaintext block(s) the operation will be performed on, likewise there is no distinction if the operation occurs one, two, or three times.

Furthermore the step of "performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of said plurality of plaintext block to produce a ciphertext block" is not operative, because the feedback operations (first, second, third?) are not well defined, in addition there is not clear understanding which plaintext block(s) the encryption operation will be performed. It appears that many errors in translation have occurred throughout claims as well as specification. After reviewing the specification pages 23-29, it appears that

more than one step essential to the operation of the method are either missing or recited in a different order than explained in the specification.

To overcome this portion of the 112 rejection all the independent claims need to be modified significantly so that missing steps are included, (i.e. counter, concatenates the series of ciphertext blocks one after another sequentially, two series of pseudo-random numbers, etc.).

8. Claims 9-12, 21-24, and 33-36 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: two computers connected over a network, padding, a pseudo-random sequences, a counter, a series of ciphertext blocks, "concatenates the series of ciphertext blocks one after another sequentially", as well as a clear explanation of what "operation(s)" are referenced in the claims. It appears that many errors in translation have occurred throughout claims as well as specification. After reviewing the specification pages 23-29, it appears that more than one step described above are either missing or recited in a different order than explained in the specification.

9. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the statutory categories of the invention.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

11. **Claims 9-12, 21-24, and 33-36** are rejected under 35 U.S.C. 102(e) as being anticipated by Shukla U.S. Patent No. 6,345,101 (hereinafter '101).

As to independent claim 9, "A symmetric-key encryption method comprising the steps of:" is taught in '101 col. 5, lines 26-32;

"dividing plaintext composed of redundancy data and a message to generate a plurality of plaintext blocks each having a predetermined length" is shown in '101 col. 3, lines 7-10;

"generating a random number sequence based on a secret key; generating a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence; outputting a feedback value obtained as a result of operation on said one of said plurality of plaintext blocks and said random number block, said feedback value being fed back for use in the operation on another one of said plurality of plaintext blocks" is disclosed in '101 col. 8, lines 56-67;

"and performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation

on still another one of the plurality of plaintext blocks to produce a ciphertext block" is taught in '101 col. 11, lines 25-35.

As to dependent claim 10, "wherein said encryption operation uses one or more said random number blocks whose total length is longer than a length of said ciphertext block" is shown in '101 col. 5, line 60 through col. 6, line 8.

As to independent claim 21, this claim is directed to the apparatus of the method of claim 9, and therefore is rejected under the same rationale.

As to independent claim 33, this claim is directed to a medium storing a program of the method of claim 9, and therefore is rejected under the same rationale.

As to dependent claims 22 and 34, these claims contain substantially similar subject matter as claim 10 and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. **Claims 11, 12, 23, 24, 35, and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over '101 in further view of Davis U.S. Patent Application Publication No. 2004/0230799 (hereinafter '799).

As to dependent claim 11, "further comprising steps of: concatenating a plurality of said plaintext blocks to generate plaintext"" is taught in '101 col. 3, lines 1-10 "The steps involved in encryption and decryption are as follows: ... Splitting of the plain-text into data blocks of fixed length. If the last data block is smaller than the desired size, it is padded with extra bits to make it the same size as the other data blocks";

The following is not taught in '101 however '714 teaches:

"extracting redundancy data included in said plaintext" in page 3, paragraphs 0030-0031 "A selected number of pseudo-random bits are extracted from pseudo-random data stream 450 in order to produce an integrity matrix 600";

"and checking said redundancy data to detect whether said ciphertext has been altered" in page 3, paragraph 0033 "The changing of a single bit of message 470 results in the changing of statistically 50% of the integrity bits, but in an externally unpredictable pattern ... and uses it to validate the incoming ICV, an attack on the message (whether in cipher-text or plaintext form)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination teachings of '101 that show a symmetric block cipher that uses multiple stages with a random number generator to include detection of tampering with the decrypted data. One of ordinary skill in the art would have been motivated to perform such a modification because digital data contains sensitive information that integrity must be protected. As indicated by '799 (see page 1, paragraph 0008-0009) "In an effort to overcome this tampering susceptibility, an integrity checksum 250 may be generated concurrently with encrypted data stream 240. Integrity checksum 250 accompanies encrypted data stream 240 ... Hence, it is

desirable to develop an efficient and cost effective technique by which various devices may securely communicate with each other with minimal latency".

As to dependent claim 12, "further comprising steps of: extracting secret data included in said plaintext; and checking said redundancy data and said secret data to detect whether said ciphertext has been altered" is taught in '799 page 4, paragraph 0037 "To establish secure communication between the two devices ... two general operations may performed; namely (1) mutual authentication and (2) production of the ICV using the shared session key".

As to dependent claims 23, 24, 35, and 36, these claims contain substantially similar subject matter as claims 11 and 12; therefore they are rejected along the same rationale.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gilgor et al. U.S. Patent Application Pub. No. 2001/0033656

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
25 May 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100